(c) Changes to existing matching programs shall be processed in the same manner as a new matching program report.

§ 310.112 Time limits for submitting matching reports.

(a) No time limits are set by the OMB guidelines. However, in order to establish a new routine use for a matching program, the amended system notice must have been published in the FEDERAL REGISTER at least 30 days before implementation (see § 310.60(f) of subpart G).

(b) Submit the documentation required by § 310.111(a) of this subpart to the Defense Privacy Office at least 45 days before the proposed initiation date of the matching program.

(c) The Defense Privacy Office may grant waivers to the 45 days' deadline for good cause shown. Requests for waivers shall be in writing and fully justified.

[51 FR 2364, Jan. 16, 1986. Redesignated at 56 FR 55631, Oct. 29, 1991, as amended at 56 FR 57801, Nov. 14, 1991]

§ 310.113 Matching programs among DoD components.

(a) For the purpose of the OMB guidelines, the Department of Defense and all DoD Components are considered a single agency.

(b) Before initiating a matching program using only the records of two or more DoD Components, notify the Defense Privacy Office that the match is to occur. The Defense Privacy Office may request further information from the Component proposing the match.

(c) There is no need to notify the Defense Privacy Office of computer matches using only the records of a single Component.

§ 310.114 Annual review of systems of records.

The system manager shall review annually each system of records to determine if records from the system are being used in matching programs and whether the OMB Guidelines have been complied with.

APPENDIX A TO PART 310—SPECIAL CONSIDERATIONS FOR SAFEGUARDING PERSONAL INFORMATION IN ADP SYSTEMS

(See paragraph (b) of § 310.13, subpart B)

A. General

1. The Automated Data Processing (ADP) environment subjects personal information to special hazards as to unauthorized compromise alteration, dissemination, and use. Therefore, special considerations must be given to safeguarding personal information in ADP systems.

2. Personal information must also be protected while it is being processed or accessed in computer environments outside the data processing installation (such as, remote job entry stations, terminal stations, minicomputers, microprocessors, and similar activities).

3. ADP facilities authorized to process classified material have adequate procedures and security for the purposes of this Regulation. However, all unclassified information subject to this Regulation must be processed following the procedures used to process and access information designated ''For Official Use Only'' (see ''DoD Freedom of Information Act Program'' (32 CFR part 286)).

B. Risk Management and Safeguarding Standards

1. Establish administrative, technical, and physical safeguards that are adequate to protect the information against unauthorized disclosure, access, or misuse (see Transmittal Memorandum No. 1 to OMB Circular A–71—Security of Federal Automated Information Systems).

2. Technical and physical safeguards alone will not protect against unintentional compromise due to errors, omissions, or poor procedures. Proper administrative controls generally provide cheaper and surer safeguards.

3. Tailor safeguards to the type of system, the nature of the information involved, and the specific threat to be countered.

C. Minimum Administrative Safeguard

The minimum safeguarding standards as set forth in paragraph (b) of § 310.13, subpart B apply to all personal data within any ADP system. In addition:

1. Consider the following when establishing ADP safeguards:

a. The sensitivity of the data being processed, stored and accessed;

b. The installation environment;

c. The risk of exposure;

d. The cost of the safeguard under consideration.